PRIVACY IMPACT ASSESSMENT (PIA)

For the

Centralized Operations Police Suite (COPS)
U.S. Army Office of the Provost Marshal General (OPMG)

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒	**Yes, DITPR**	Enter DITPR System Identification Number	2822 (DA08154)
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☐	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI 007-21-01-20-02-2259-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier A0190-5 OPMG; A0190-45OPMG; A0190-47 DAMO; A0190-9 OP

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 951
10 U.S.C. 3013
18 U.S.C. 44, Brady Handgun Violence Prevention Act
28 U.S.C. 534, Uniform Crime Reporting Act
42 U.S.C. 10606, Victims Rights and Restitution Act of 1990

E.O. 9397 (SSN).

Status of Forces Agreement between the United States of America and the host country in which U.S. Forces are located

DoD Directive 10310.1, Victim and Witness Assistance

Army Regulation 190-9, Absentee Deserter Apprehension Program and Surrender of Military Personnel to Civilian Law Enforcement Agencies
Army Regulation 190-13, The Army Physical Security Program
Army Regulation 190-14, Carrying of Firearms and Use of Force for Law Enforcement Security Duties
Army Regulation 190-45, Military Police Law Enforcement Reporting
Army Regulation 190-47, The Army Corrections System

Army Regulation 195-2, Criminal Investigation Activities
Army Regulation 380-13, Acquisition and storage of Information Concerning Non-Affiliated Persons and Organizations
Army Regulation 630-10, Absence Without Leave, Desertion, and Administration of Personnel Involved in Civilian Court Proceedings

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The COPS is a centralized database that contains five subsystems that support the Army Military Police Corps. These subsystems provide (1) law enforcement reporting via the Military Police Reporting System (MPRS); (2) correctional tracking via the Army Correctional Information System (ACIS); (3) vehicle and weapons registration via the Vehicle Registration System (VRS); (4) enemy prisoner of war and detainee accountability via the Detainee Reporting System (DRS); and (5) parole and clemency management of inmates in Army correctional institutions which is the Army Review Board Agency (ARBA).

The system contains data derived from military police reports and or similar reports containing investigation of criminal complaints and incidents in which there is an Army interest, along with details of any criminal prosecution, civil court action, or non-judicial administrative punishment. The system also records the registration of vehicles and weapons. In addition, the system contains details from correctional treatment records which are used to determine prisoners' custody classifications, work assignments, educational needs, adjustment to confinement, areas of particular concern, and, as the basis for clemency, parole and restoration to duty considerations. Automated records provide pertinent information required for proper management of confinement facility population, demographic studies, status of discipline and responsiveness of personnel procedures, as well as confinement utilization factors such as population turnover, recidivism, etc. The system contains information on agency personnel as well as members of the public, family members, victims and witnesses of crimes. The system assists the Army in maintaining discipline, law and order, and aids law enforcement and criminal intelligence personnel in executing the law. The system provides management data on which to base crime prevention, selective enforcement, and improved driving safety. The system also provides statistical data for the purposes of developing crime trends by major categories (e.g., crimes against persons, drug crimes, crimes against property, fraud crimes and other offenses); developing law enforcement and crime prevention programs to reduce or deter crime within Army communities; to satisfy statutory reporting requirements; and in support of Army safety programs.

The COPS is an existing system in Operations and Maintenance (O&M) life-cycle management and is owned by Office of the Provost Marshal General. The system presently has no boundaries and interconnections with any other systems.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Due to the stringent level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing individuals the opportunity to object or consent.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. Action Commanders, Staff Judge Advocates, Intelligence agencies, Morale and Welfare activities, Army & Air Force Exchange Service, Army Staff Principals in the chain of command, Department of the Army Inspectors General, Army Audit Agency, Army Criminal Investigation Command, Army Intelligence and Security Command, Provost Marshal General, Assistant Secretary of the Army (Financial Management & Comptroller), medical facilities, Army Agencies authorized to obtain information for employment and other security concerns, and to Commanders and their designated personnel responsible for implementing disciplinary and prosecutorial actions.

☒ **Other DoD Components.**

Specify. DOD Inspector General, Defense Criminal Investigative Service, Air Force Office of Special Investigations, Navy Criminal Investigative Service, Defense Finance and Accounting Service, and medical facilities.

☒ **Other Federal Agencies.**

Specify. Office of Management and Budget, Department of Veterans Affairs, other federal law enforcement and confinement/correctional agencies; Bureau of Prisons, Alcohol, Tobacco & Firearms, Federal Bureau of Investigation, Office of Personnel Management, Department of Homeland Security, Federal child protection services or family support agencies, Immigration and Naturalization Services, Department of Justice, Internal Revenue Service, General Services Administration, National Archives and Records Administration, the Merit Systems Protection Board, and the Office of Special Counsel.

☒ **State and Local Agencies.**

Specify. State and local law enforcement agencies, motor vehicle departments, state & local confinement/correctional facilities, medical facilities, state and local child protection services and family support agencies.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Lockheed Martin Information Technology

COPS operations and maintenance life-cycle management is maintained by Contract support. The contract states that all contract personnel assigned to the contract shall hold a Secret clearance. All information available to the contractor while performing this task, both electronic or otherwise, should be maintained in a strictly confidential manner and protected in accordance with its designated security classification. Contractor personnel performing work on this task order must comply with AR 25-2 Information Assurance, Section 5, Personnel Security. The security designation for IT and IT-related positions states that contractor personnel will possess the favorable completion of a National Agency Check (NAC) current within 180 days, Single Scope Background Investigation (SSBI) or favorable review of SF85P, SF86, and Supplemental Questionnaire.

Contractors who work at Installation Provost Marshal Offices army-wide has access to COPS, specifically vehicle registration offices.

☒ **Other** (e.g., commercial providers, colleges).

Specify. Limited information may be provided to victims and witnesses of crimes, limited information may be disclosed to foreign counties under the provision of the Status of Forces Agreements, or Treaties.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to object. Individuals may refuse to cooperate with the investigation as long as the actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters USACIDC or the Army Board of Correction of Military Records.

(2) If "No," state the reason why individuals cannot object.

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to object. Individuals may refuse to cooperate with the investigation as long as the actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters USACIDC or the Army Board of Correction of Military Records.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

Given the nature of Law Enforcement responsibilities and undercover operations, suspects and subjects are not always given the opportunity to give or withhold their consent. Individuals may refuse to cooperate with the investigation as long as the actions do not obstruct justice. Erroneous records may be expunged or corrected by request to Headquarters USACIDC or the Army Board of Correction of Military Records.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒	**Privacy Act Statement**	☒	**Privacy Advisory**
☒	**Other**	☐	**None**

Describe each applicable format.

A Privacy Act Statement is furnished to individuals at the time data is collected on the DA Form 2823, Sworn Statement, DA Form 3975, Military Police Report, and DA Form 3946, Military Police Traffic Accident Report. Also, individuals are provided rights under the DA Form 3881, Rights Waiver.

DA Form 2823:
Information provided may be further disclosed to federal, state, local, and foreign government law enforcement agencies, prosecutors, courts, child protective services, victims, witnesses, the Department of Veterans Affairs, and non-judicial punishment, other administrative disciplinary actions, security clearances recruitment, retentions placement, and other personnel actions.

DA Form 3881:
Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval. Disclosure of you Social Security Number is voluntary.

DA Form 3975:
Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval. Disclosure of you Social Security Number is voluntary.

DA Form 3946:
Your Social Security Number is used as an additional/alternate means of identification to facilitate filing and retrieval. Disclosure of you Social Security Number is voluntary.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.